Claims

1. Data processing device (MOB1) which can communicate with a number of sets of resources (WEB1,WEB2) via a browser (BW1), characterised in that the browser (BW1) comprises a number of private zones (ZP1-ZP2), where each private zone can be allocated to a respective set of resources (WEB1) to store information, said device comprising a plug-in (VBA) ensuring that a set of resources (WEB1) communicates exclusively with the private zone (ZP1) allocated to it.

2. Device according to claim 1, characterised in that said plug-in (VBA) comprises at least one input parameter (USERID,PW) corresponding to a zone access key, the value of this access key being supplied through a secured transmission by the set of resources concerned (WEB1) to said device, said plug-in, after execution and depending on the key, being able to authorise access to a private zone (ZP1), and deny access to the other private zones (ZP2) of said browser (BW1).

3. Device according to claim 1 or 2, characterised in that, for the authentication step, the set of resources (WEB1) transmits a request to the browser prompting the user to enter an access key (USERID, PW) received, and in that if the access key is correct, the plug-in (VBA) comprises code instructions which can manage the authentication between a set of resources (WEB1) and the corresponding allocated private zone (ZP1).

4. Device according to claim 1, characterised in that each zone (ZP1-ZP2) can store information, in particular security information ensuring secured communication between a private zone (ZP1) and a set of resources (WEB1).

5. Device according to claim 1 or 4, characterised in that it interprets code instructions which, after the authentication step and using security information

stored in the private zone concerned, can manage the administration of the private zones as well as the use of application data in these private zones during a communication between the browser and the set of resources (WEB1).

6. Computer resource (WEB1), in particular a WEB site, communicating with a data processing device (MOB1) via a network, characterised in that said device includes a browser (BW1) as defined in claim 1, and in that said computer comprises a plug-in which, when executed, can obtain the allocation of a private zone (ZP1), said allocation ensuring that the communication between said private zone (ZP1) and said resource (WEB1) is exclusive.

7. Resource according to claim 6, characterised in that the private zones are managed by an entity (OP), and in that this entity (OP) allocates a private zone (ZP1) to a resource (WEB1), said entity transmitting to said resource security parameters, in particular parameters which can identify the allocated private zone (VAS id).

8. Resource according to claim 7, characterised in that said entity transmits to said resource at least one master key (VMK) previously stored in the allocated private zone, said key being able to encrypt information transiting between said zone and the set of resources.

9. Resource according to claim 6, characterised in that it comprises secured means to transmit to said device a key (PW,USERID) to access a private zone, said device using this key, during communication between said resource and said device, to authenticate the private zone with the computer resource (WEB1).

10. Manager (OP), in particular an operator, which can manage the use of said device as defined in claim 1, characterised in that it comprises a plug-in which can manage, upon request, the allocation of a private zone (ZP1) to a set of

resources by supplying to said set of resources information comprising at least the reference (VASId) of a private zone (ZP1).

11. Smart card (CARD1) which can communicate with a number of sites (WEB1) via a browser (BW1), characterised in that:

- the browser comprises a number of private zones (ZP1-ZP2), where each private zone can be allocated to a respective set of sites and can store security information ensuring secured communication with a set of sites;

- and in that the browser (BW1) interprets code instructions ensuring that a set of sites (WEB1) communicates exclusively with the private zone (ZP1) allocated to it.

12. Communication method between a data processing device (MOB1) comprising a browser (BW1) and a set of resources (WEB1), characterised in that it comprises the following steps:

- a step to create, in said browser, a number of private zones (ZP1-ZP2), where each private zone can be allocated to a respective set of resources and can store security information ensuring secured communication between said private zone and a set of resources;
- a step to allocate a private zone (ZP1) to a set of resources (WEB1),
- a step to communicate between said allocated private zone (ZP1) and the set of resources concerned (WEB1), a plug-in denying access during this communication to any private zone other than the allocated zone (ZP1).

13. Method according to claim 12, characterised in that the allocation of a private zone (ZP1) is managed by an entity (OP), and in that this entity allocates a private zone (ZP1) of the card (CARD1) to the set of resources (WEB1) by supplying information comprising in particular the reference (VASId) of the allocated private zone (ZP1).

14. Method according to claim 13, characterised in that the information comprises the value of a master key (VMK) previously stored in the corresponding private zone (ZP1), this key being able to encrypt information transiting between said zone and the set of resources during a communication.

15. Method according to claim 12, characterised in that the set of resources (WEB1) transmits by a secured transmission means at least one access key (USERID,PW) associated with a private zone (ZP1), said key being used to execute a plug-in able, after execution, to authorise access to a private zone (ZP1) and deny access to the other private zones (ZP2).

16. Method according to claim 12, characterised in that, in order to open a secured transaction, the set of resources (WEB1) transmits a plug-in which can check whether the security information written in the private zone (ZP1) corresponds to the security information stored in a memory attached to the set of resources (WEB1).

17. Computer plug-in (VBA) for a data processing device (MOB1) which can communicate with a number of resources (WEB1,WEB2) via a browser (BW1), characterised in that the browser comprises a number of private zones (ZP1-ZP2), where each private zone (ZP1) can be allocated to a respective set of resources (WEB1) and can store information specific to this set of resources (WEB1), and in that the plug-in comprises at least one input parameter corresponding to a key (USERID,PW) to access a zone, the value of this key being supplied to said device by the set of resources concerned, said plug-in, after execution and depending on this key, being able to authorise or deny access to a private zone and deny access to the other private zones if the access is authorised.

18. Computer program (OPG) stored in a manager entity (OP) which can manage private zones as defined in claim 1, the purpose of said program being,

when it is executed on said entity, to allocate a private zone (ZP1) of said browser (BW1) to a set of resources (WEB1) by supplying information including at least the reference (VASId) of the private zone (ZP1).